INFORMATION ASSET SECURITY CLASSIFICATION POLICY

Status:	Active Policy
Effective Date:	April 5, 2007 through April 4, 2009
Revised Date:	N/A
Approved By:	J. Stephen Fletcher, CIO
Authority:	*UCA §63F-1-103; UCA §63-2-201; Utah Administrative Code, R895-7 Acceptable Use of Information Technology Resources; Utah Administrative Code, R477-11 Discipline*

2.1 PURPOSE

This policy defines an impact-based asset classification framework for the functional security requirements of all information assets owned, processed, stored, or transmitted by the Department of Technology Services (Department).

2.1.1 Background

On December 11, 2001, the Governor of Utah issued an executive order directing the Chief Information Officer (CIO) to develop and implement policies that promote the security of State information and information systems. The CIO has determined that information security is an issue for all state agencies, and the Department of Technology Services (DTS) will assist agencies to govern and protect their information assets.

The protection of information assets owned, processed, stored, or transmitted by a state agency requires the use of security controls that are based on business rules which govern access. As the steward of information assets, each state agency must identify the appropriate level of protection for any given information asset. DTS will assist each asset steward to develop and implement security controls based on business rules which govern access and provide sufficient protection for each information asset.

2.1.2 Scope

This policy applies to all information assets owned by the Department of Technology Services.

2.1.3 Exceptions

None, unless otherwise specified within this policy

2.2 DEFINITIONS

Accessibility
A functional security requirement used to determine how an information asset can be accessed.

Asset Manager
A DTS employee authorized by an Asset Steward and the CIO to manage state information assets.

Asset Owner
A government entity recognized or identified by the State of Utah as an actual or potential owner of real, personal, or intellectual property. For the purposes of this policy, the Asset Owner of Department property is the CIO.

Asset Steward
A DTS employee recognized or identified by the CIO as the steward of Department property.

Availability
A functional security requirement used to determine when an information asset must be accessible.

Confidentiality
A functional security requirement used to determine how an information asset can be disclosed.

Government Information Asset
Information that is prepared, owned, received, or retained by a governmental entity that in its original form is reproducible by mechanical or electronic means.

Integrity
A functional security requirement used to determine how an information asset can be altered, destroyed or modified.

Public Information Asset
A Department information asset that is not private, controlled, or protected and that is not exempt from disclosure as provided in the Utah Government Records Access and Management Act.

Security Risk Assessment
The process of identifying risks to agency assets or agency operations (including mission, functions, image, or reputation) by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate the impact.

2.3 POLICY

All information assets owned, processed, stored, or transmitted by the Department are to be classified by the asset owner or steward according to the functional security requirements of the asset and the impact to the State, Department, or an individual if those requirements are not met. These classifications are to be used in determining the allocation of resources as well as the formulation of controls to mitigate the possible compromise of the functional security requirements.

2.3.1 Security Impact Levels

Given that information asset classification is based upon security impacts to the State, agency, or an individual, it becomes necessary to define a common set of security impact levels. There are five security impact levels: None, Low, Moderate, High, and Critical.[1] The following items are to be considered when defining a security impact level:

- As security impact levels increase, the potential costs of mitigating those impacts increase as well; and
- Statutes, rules, or other special agreements may mandate the use of specific security impact levels.

2.3.1.1 Impact Level: None

The potential security impact is NONE if a compromise of the functional security requirement is expected to result in no adverse effect on organizational operations, organizational assets, or the physical or financial well-being of an individual.

2.3.1.2 Impact Level: Low

The potential impact is LOW if a compromise of the functional security requirement is expected to have a limited adverse effect on organizational operations, organizational assets, or the physical or financial well-being of an individual.

Examples of limited adverse effects include:

- Degradation in mission capability to an extent and duration that the organization is able to perform its primary business functions, but the effectiveness of the functions is noticeably reduced.
- Minor damage to organizational assets.
- Minor financial loss by the organization.
- Minor physical or financial harm to an individual.

2.3.1.3 Impact Level: Moderate

The potential impact is MODERATE if a compromise of the functional security requirement is expected to have a serious adverse effect on organizational operations, organizational assets, or the physical or financial well-being of an individual.

Examples of limited adverse effects include:

- Significant degradation in mission capability to an extent and duration that the organization is able to perform its primary business functions, but the effectiveness of the functions is significantly reduced.
- Significant damage to organizational assets.
- Significant financial loss by the organization.

[1] See Appendix 1 for an explanation and examples of security impacts.

- Significant physical or financial harm to an individual, but does not involve the loss of life or serious life threatening injuries.

2.3.1.4 Impact Level: High

The potential impact is HIGH if a compromise of the functional security requirement is expected to have a severe adverse effect on organizational operations, organizational assets, or the physical, financial, or emotional well-being of an individual.

Examples of limited adverse effects include:

- Severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary business functions.
- Improper disclosure of financial system information.
- Improper disclosure of information governed by the Privacy Act of 1974
- Severe damage to or loss of organizational assets.
- Severe financial loss by the organization.
- Significant financial loss by the state.
- Severe financial harm to an individual.
- Severe physical harm to an individual, with the potential for the loss of life or other serious life-threatening injuries.

2.3.1.5 Impact Level: Critical

The potential impact is CRITICAL if a compromise of the functional security requirement is expected to have a catastrophic effect on statewide operations or to an individual which will result in the loss of life.

Examples of limited adverse effects include:

- Catastrophic loss of mission capability to an extent and duration that the State is not able to perform one or more of its primary business functions.
- Catastrophic damage to or loss of organizational assets.
- Catastrophic financial loss by the organization.
- Severe or catastrophic financial loss by the State.
- Severe or catastrophic financial harm to an entire class of persons.
- An expectation for the loss of one or more lives.

2.3.2 Classification of Information Assets

The security classification of an information asset must be based on the asset's functional security requirements.

2.3.2.1 Each functional security requirement will receive a unique designation. The designation of one functional security requirement does not determine the designation of other functional security requirements for the same asset.

2.3.2.2 At a minimum, every information asset has four functional security requirements that must be defined and classified. These functional security requirements are Accessibility, Confidentiality, Integrity, and Availability.

2.3.2.2.1 Functional security requirements must be defined in a timely manner by the asset steward or the asset steward's designee. The Chief Information Security Officer (CISO) shall provide sufficient information and resources to support the asset steward's or designee's effort to define and classify the functional requirements of an information asset.

2.3.2.2.2 If the asset steward or designee fail to define the functional requirements for an information asset in a timely manner, the Department of Technology Services may define the functional security requirements for the information asset as None.

2.3.2.3 To ensure the security classification of an information asset is current and reflects the asset owner's requirements, the classification will be reviewed:

- Annually;
- Whenever there has been a change to the information asset's functional security requirements; or
- Whenever there has been a significant change to the information asset's business requirements (e.g., accessibility, availability, confidentiality, integrity).

2.4 APPENDICES

- Sample Asset Classification
- Nation Institute of Standards and Technology (NIST) Special Publication 800-60, version 2.0; Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories. (Available at: http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf)

DOCUMENT HISTORY

Originator:	J. Stephen Fletcher, Chief Information Officer
Next Review:	February 20, 2009
Reviewed Date:	N/A
Reviewed By:	N/A